# Analysis for System Safety

Friday, August 20, 2004

Presented by AFS-900

# Topics

- Systems
  - The processes
  - The Environment
- System Evaluation
  - Safety Process Mapping

# What's a System?

*"A system is a composite of people, tools, procedures, materials, equipment, facilities, and software operating in a specific environment to perform a specific task or achieve a specific purpose, support, or mission requirement."*

- Roland and Moriarty, System Safety Engineering and Management

Systems

People

Tools

Procedures

Software

Equipment

Facilities

Materials

...a set of components
that act together as a whole
to achieve a common goal

# Processes

- A set of interrelated activities that convert inputs into outputs (ISO 9000-2000)

*If you can't describe what you're doing as a process you don't know what you're doing.*

*-W. Edwards Deming*

# Organizational Systems

- Aviation Systems (AS) are *Organizations*
- Their primary components are *People*
- Their processes are the sets of *Activities* that the people perform to accomplish the organization's goals
- Their *Structures* are the manner in which their people interact and how they do their jobs
- This necessitates an *Organizational Focus* to analysis and management of the system

# Operational Environments

- Each system operates in a specific environment
- Environments include:
  - The physical environment
  - The business and economic environment
  - The national and cultural environment
  - The resource environment
  - The regulatory environment
- Systems must continually adapt to changes in their environment to operate efficiently, profitably, and safely

# Open Systems

- The modern aviation system is characterized by:
  - Environmental complexity
  - Environmental turbulence
- Change is constant, frequent, and significant
- Adaptation of the productive system to the market environment is a recognized business reality
- Adaptation of the safety system to the current operational environment is also necessary

# Aviation Systems - Production

- Aviation systems are the systems that convert inputs to outputs to provide goods and services to customers
- Productive systems also consume resources and work in defined, sometimes rapidly changing business and operational environments
- Modern aviation systems are often complex, frequently changing networks of suppliers and other service providers, e.g.:
  - Contract maintenance and training
  - Ramp services
  - Engineering and technical services
  - Code shares, wet leases and alliances
  - Business support (e.g. IT, admin)

# Oversight Systems - Protection

- Basic Compliance – Quality Control (QC)
- System Safety – Process/Quality Assurance (QA)
  - Regulatory Components
  - Voluntary Components
- Traditional oversight systems stressed external (FAA) oversight and a “one size fits all” compliance approach
- Future oversight must be collaborative and tailored to system needs

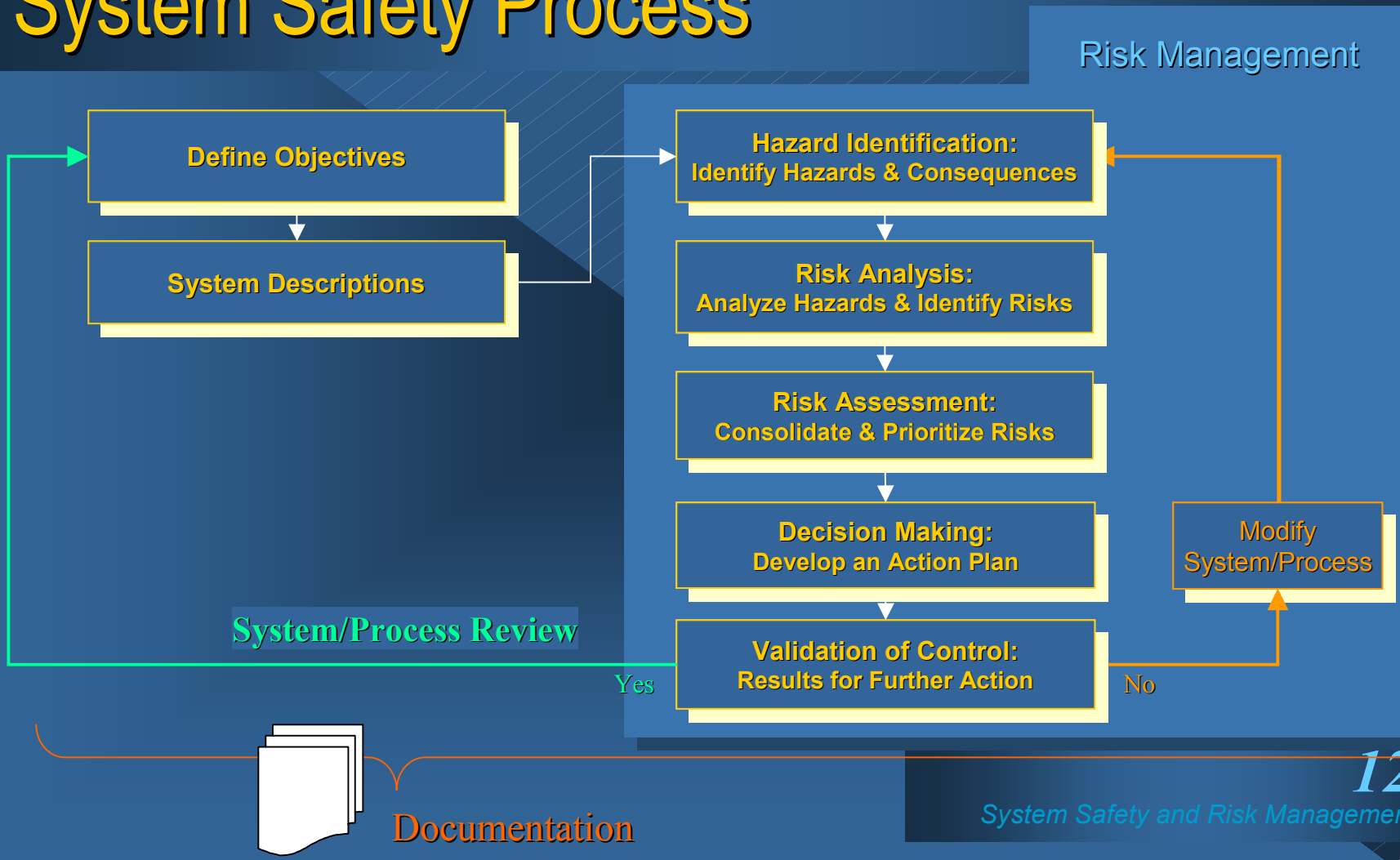
# Safety and Quality

- Safety is an an outcome of an organization's processes
- "Safety management" is really the result of management of process quality
- Managing the fundamental properties of process quality is the key to safety

# Why Do System Safety?

- Air traffic is increasing
- Aviation operations are becoming more complex
- FAA oversight staff and resources are constrained
  - *We can no longer afford to function as a direct source of QC*
- Systems approach is proactive -
  - *Stresses process improvements*
- System safety is good business

# System Safety Process



# Regulations and System Safety

- The objective of the regulatory process is to enhance safety
- Regulations provide requirements for expected conduct of operations
- Regulations serve as risk controls
- It's not only if the regulations are applied but how they are applied that can make a difference

# Types of Oversight

- Traditional:
  - Compliance orientation
  - Certification of organizations and key programs
  - Sampling of operations
  - Currently covers most certificate holders
- System Safety Methods:
  - First generation SS – ATOS
  - Compliance is a means to an end
  - Transitional System – SEP
  - SEP for smaller operators under development in Alaskan Region

*"Accidents Are Not Due to Lack of Knowledge, but Failure to Use the Knowledge We Have."*

- Trevor Kletz, "What Went Wrong?"

# Knowledge requirements

- What do I need to do?
- What do I need to know?
- How do I tell if it's happening?

# Types of System Evaluation

- Situational Risk Analysis
  - Detecting hazards in the operating environment.
- Design
  - Quality and compliance built in.
- Performance
  - Compliance with the design (Are they doing it?).
  - Effectiveness of the design (Does it work?).
- Diagnosis
  - Finding causes and cures for identified problems.

# Situational Risk Analysis

- Uses Risk Indicators
  - Impacts on system assessed
- Tools provided to assess system risk and develop surveillance plans.
  - ATOS – ACAT, RMP
  - SEP – SEAT, Risk Worksheets
- Others – apply the System Safety/Risk Management process

# System Design Evaluation

- Based upon six attributes
- Derived from quality, systems engineering, safety literature
- Primary tool (air carrier) is Safety Attribute Inspection (SAI)
  - Data recorded in ATOS D/R or PTRS
- Many certification and tech admin activities also evaluate and document system design
- Used as an initial and periodic comprehensive audit

# ATOS Systems & Sub-Systems

| Aircraft Configuration Control | Manuals | Flight Operations | Personnel Training & Qualifications | Route Structure | Flight, Rest, & Duty Time | Technical Administration |
|---|---|---|---|---|---|---|
| Aircraft | Manual Requirements | Programs & Procedures | Maintenance Personnel Qualification | Approved Routes & Areas | Airman & Crew Limitations | Key Personnel |
| Records & Reports | | Dispatch & Release | Training Programs | | Maintenance Personnel | Other Programs |
| Organization | | | Crew & Dispatch Qualifications | | | |
| | | | Mechanic & Repairman Certification | | | |

# Air Carrier Operations System Model (ACOSM) Systems and Subsystems

| System Management | Flight Operations | Maintenance Inspection Engineering | Training (Maintenance, Crew, Other) | Resource Management |
|---|---|---|---|---|
| Planning | Passenger Services | Maintenance Management & Control | Training Requirements Management | Resource Requirements Analysis |
| Policy & Procedure Development | Cargo Handling | Maintenance Quality Assurance | Training Design & Development | Resource Control & Procurement |
| Operational Control | Ground Operations & Services | Aircraft Maintenance | Training Delivery | Material Handling & Distribution |
| Information Management | Aircraft Operations | Engineering Support | Training Evaluation | Human Resource Management |

# Performance Evaluation

- Evaluation designed to tell if:
  - The system is being used as designed and
  - If it is effective
- Primary tool is Element Performance Inspection (EPI)
  - Data recorded in ATOS D/R or PTRS
- Many surveillance and investigatory activities also provide data on system performance

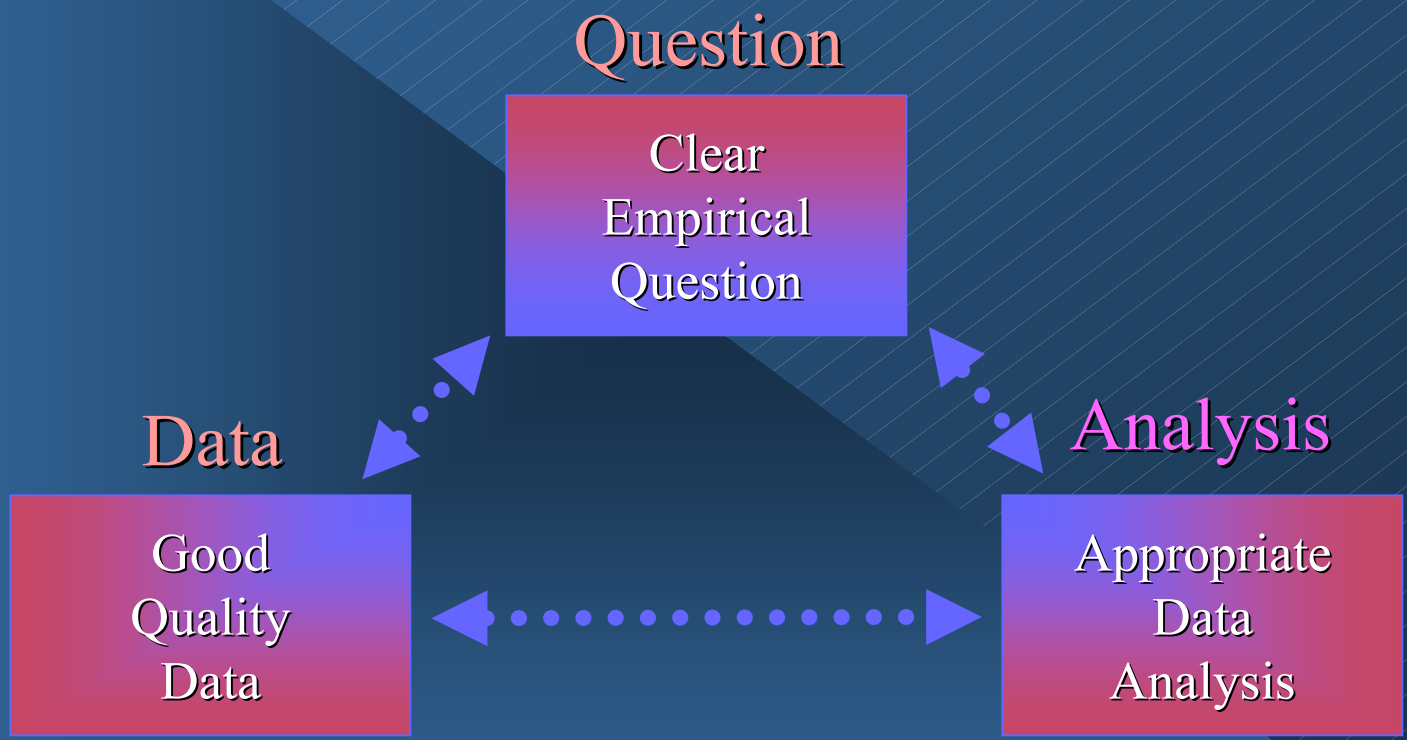
# Diagnosis

- Analytical Process
  - ORA's at CMT's
  - FSAIC supporting
- Additional Tools
  - Risk Management Plans (ATOS)
  - Risk Worksheets (non-ATOS)

*Data is like garbage, you'd better know what you're going to do with it before you collect it.*

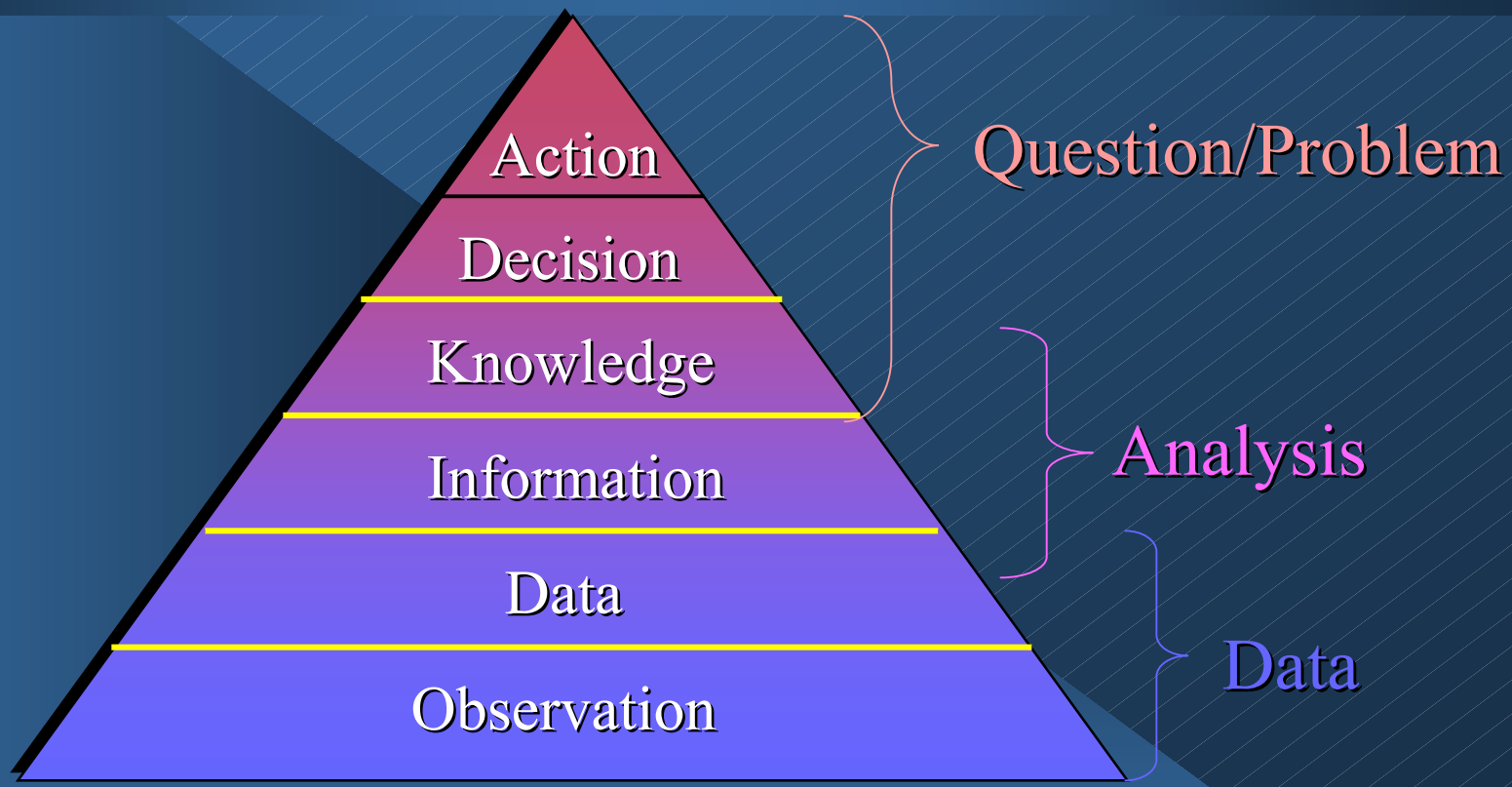
*Mark Twain*

# The Analysis Triangle

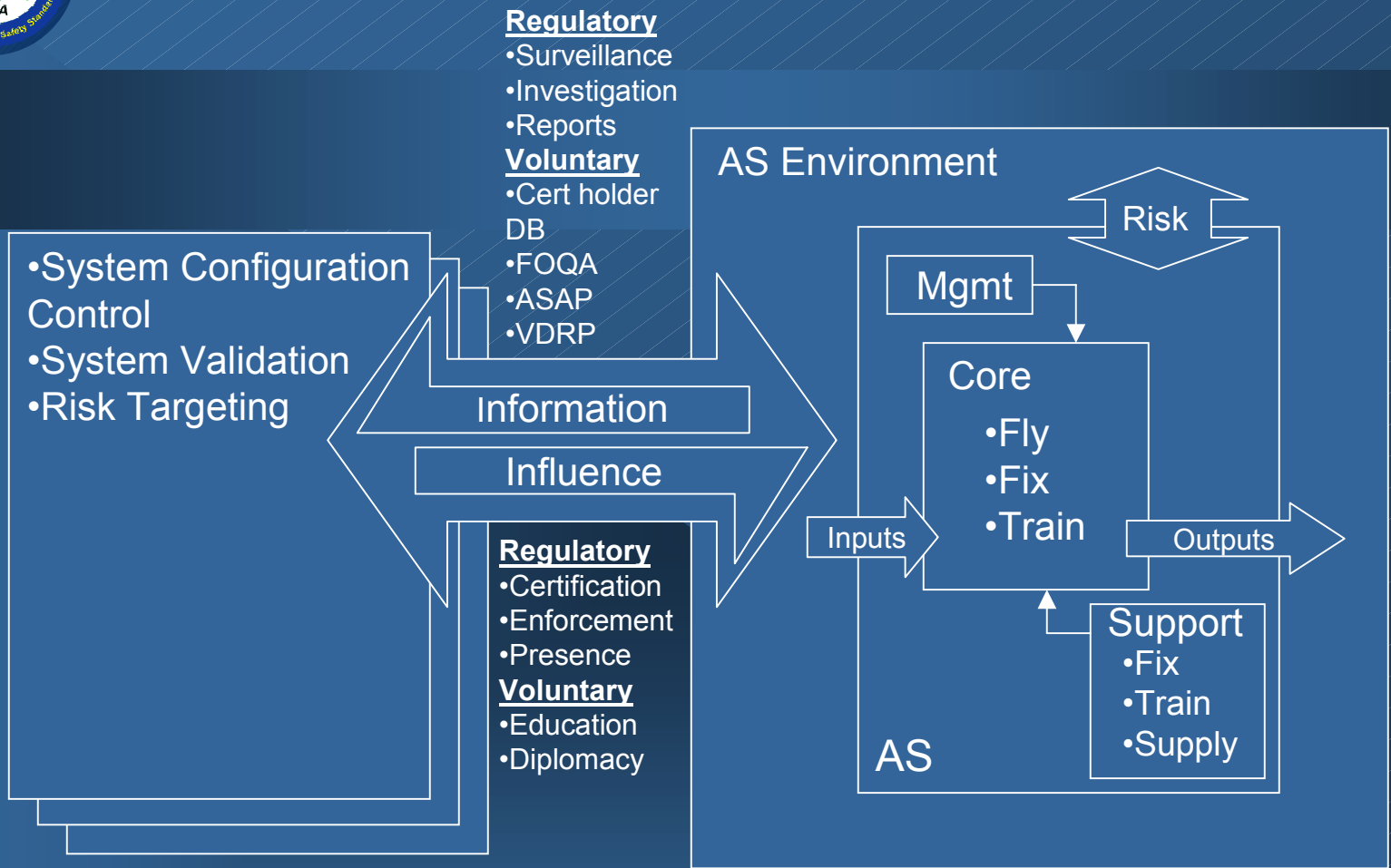



Source: *Dr. Robert Holt*

# Decision-Making Hierarchy



# Aviation Safety Oversight Processes



For additional information contact:

FSAIC

Don Arendt
Manager, Flight Standards Safety Analysis Information Center
(703) 661-0516 don.arendt@faa.gov

Tim Liddle
Operations Research Analyst, SWA-CMO
(214)277-0206 timothy.i.liddle@faa.gov

*Layout Designed by ~C.Werlhof*